

External Enumeration and Exploitation of Email and Web Security Solutions

Ben Williams



About this talk

- Background
- Enumerating web filtering solutions
- Enumerating email filtering solutions
- Bypassing filters



Previous presentations (Hacking appliances)

- Blackhat EU 2013 – Hacking Security Appliances
- <http://www.youtube.com/watch?v=rrjSEkSwwOQ>

- Blackhat Webcast July 2013 – Hacking Security Appliances
- <http://www.blackhat.com/html/webcast/07182013-hacking-appliances-ironic-exploits-in-security-products.html>

- BlackHat EU 2012 - Exploiting Security Gateways via their Web UIs
- <http://www.youtube.com/watch?v=XfZS1iZ2PpY>



Previously (Hacking appliances/gateways)

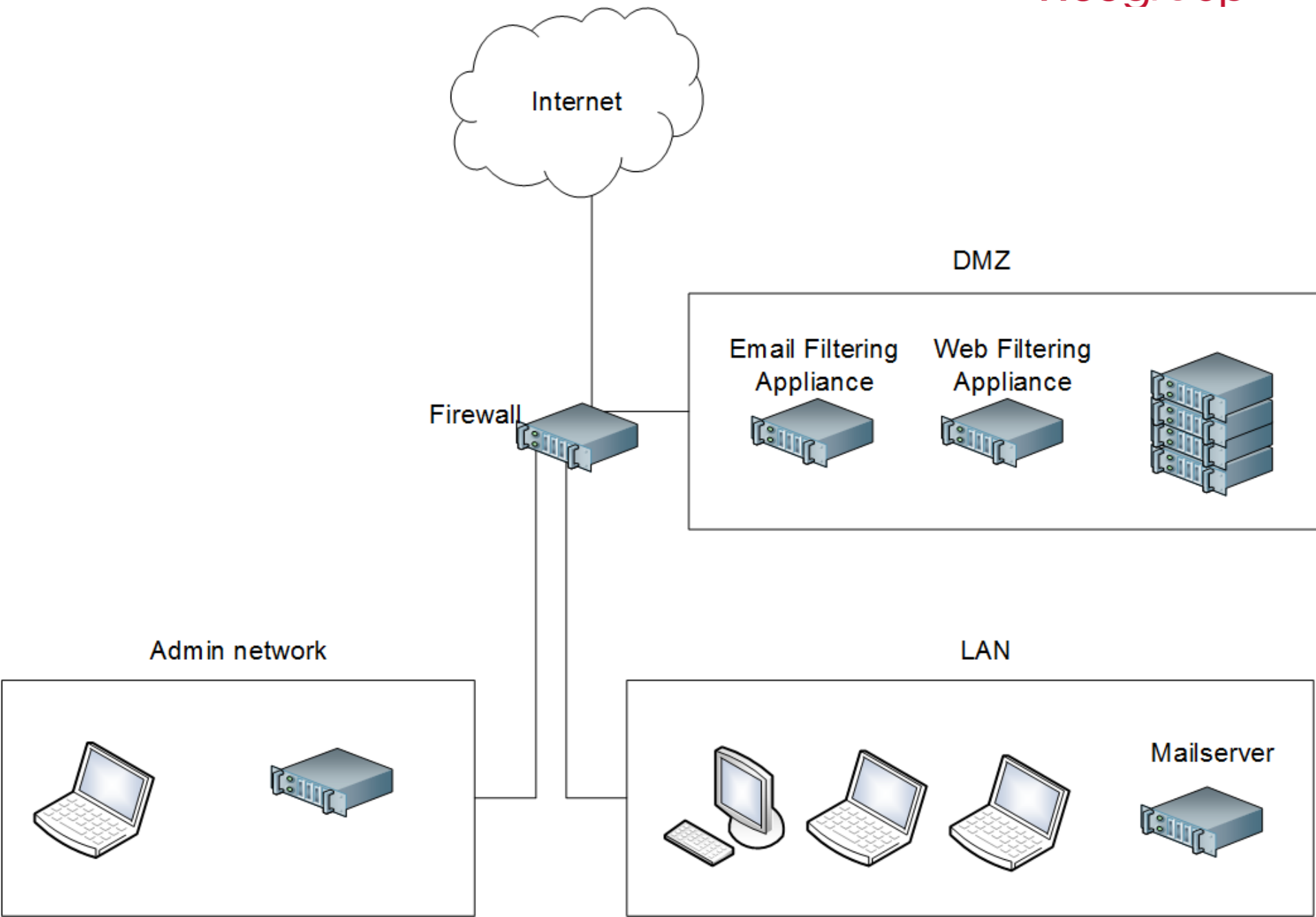
- Email/Web filtering
 - Baracuda, Symantec, McAfee, Trend Micro, Sophos, Proofpoint
- Firewall, Gateway, Web-filters
 - Pfsense, Untangle, ClearOS, Websense, Citrix



Research this time - Enumeration

- Enumerating and bypassing products and solutions
- Low severity issues which are systemic and persistent
- Using functionality which is there by design





For an attacker: Wouldn't it be good if ?...

- Vulnerability scanning
 - Hidden vulnerable products could be detected externally
- Phishing and client-side attacks
 - Clear picture of defences before targeting real users
- Email or Web filter policy, or product capability review
 - Automated and remote testing



MailFEET and WebFEET usage to date

- Detailed analysis during NCC Group customer engagements
- Targeting specific products in a test environment
 - To identify product capability and weaknesses
- Limited payloads and tests of a wide variety of domains
 - To improve the tool and produce some stats

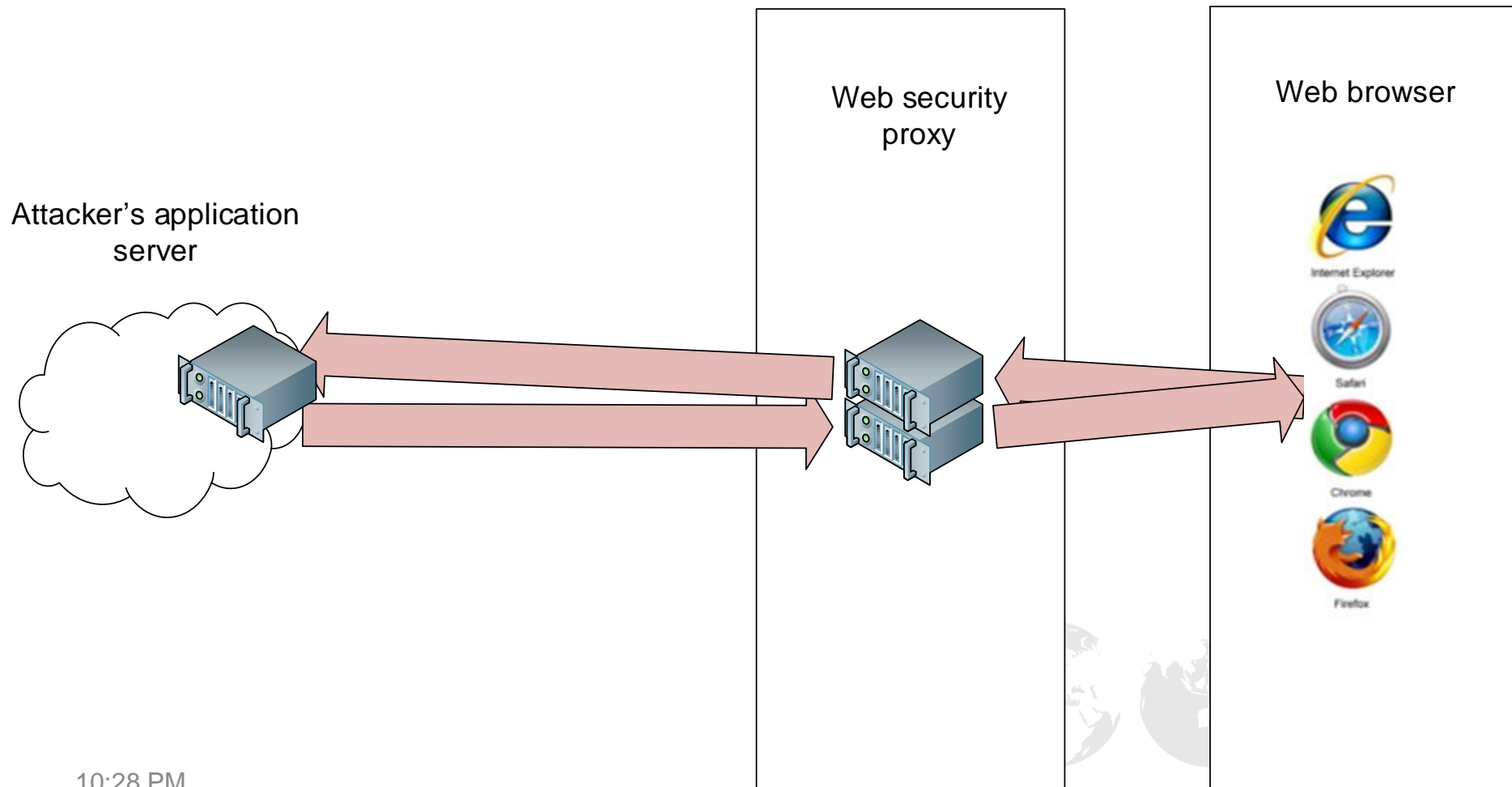


WebFEET

- Web Filter External Enumeration Tool (WebFEET)
- Drive-by web-proxy and policy enumeration with JavaScript
- Main components (HTML, JavaScript, PHP)
 - Enumerates proxies
 - Simulates download of files
 - Uploads a report
- For audits and reconnaissance



Header Modification Enumeration

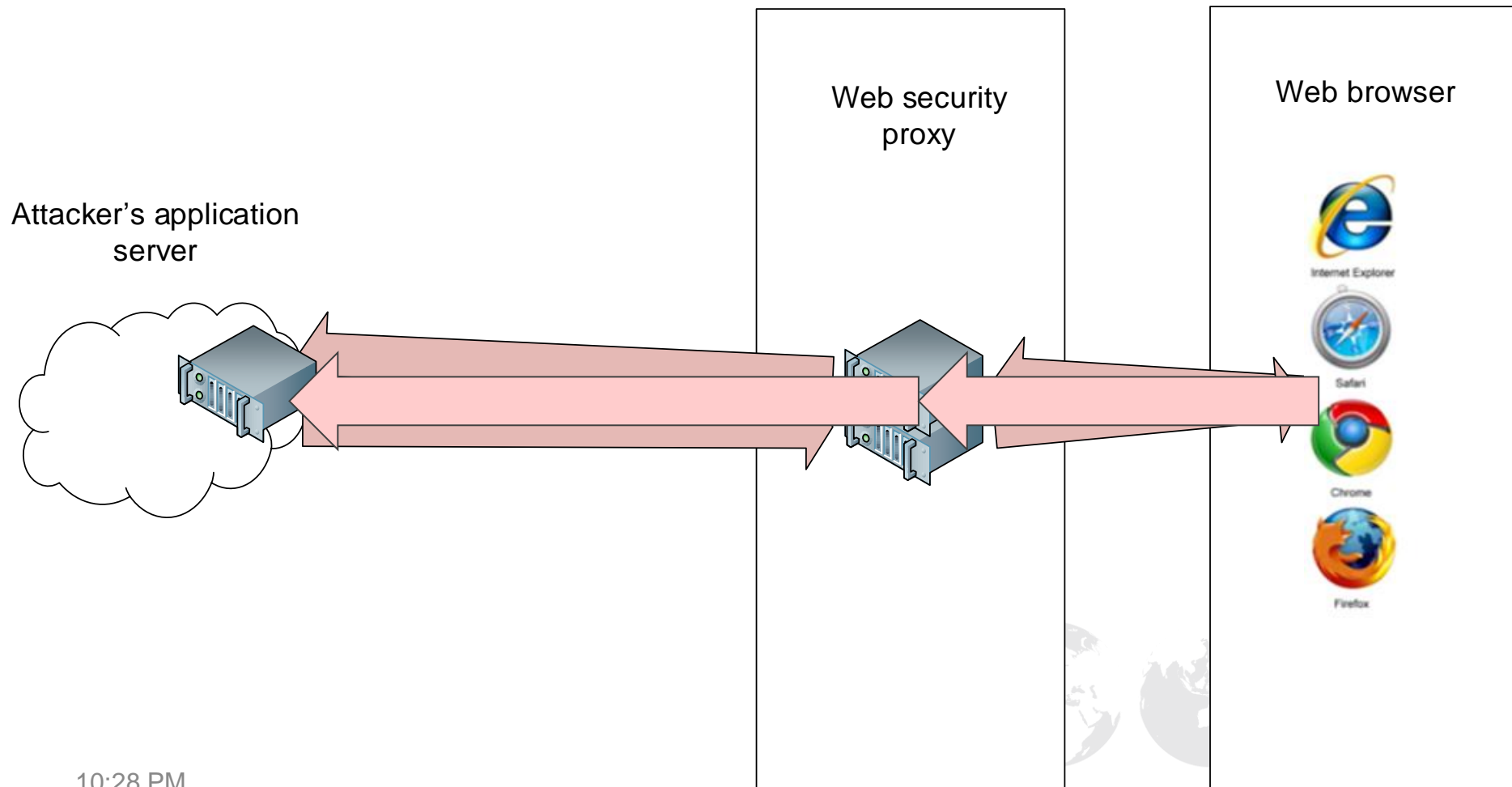


Web filter IP address/hostname/version

```
HTTP/1.1 200 OK
Date: Thu, 12 Jun 2014 13:26:33 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Thu, 13 Mar 2014 20:08:22 GMT
ETag: "1c0a6f-4ab-4f48283e160cb"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 1195|
Content-Type: text/html
X-Cache: MISS from ipfire.localdomain
X-Cache-Lookup: MISS from ipfire.localdomain:800
Connection: keep-alive
```



Header Modification Enumeration



Web filter IP address/hostname/version

- Interesting headers
 - Via
 - X-Cache
 - X-Cache-Lookup
 - Other customer X-headers
 - Subtle modifications



Collected Headers Examples

X-Cache-Lookup: MISS from wp-xxxxxxx.xxx.xx.xx:3128

X-Cache: MISS from 10.xx.xx.xx

Via: 1.0 10.xx.xx.xx (McAfee Web Gateway 7.2.0.1.0.13253)

Via: 1.0 barracuda.xxxxxxxxxxxxxx.xx:8080 (http_scan/4.0.2.6.19)

Via: 1.1 xxxproxy02.xx.xxxxxx.com:3128 (Cisco-IronPort-WSA/7.5.2-118)

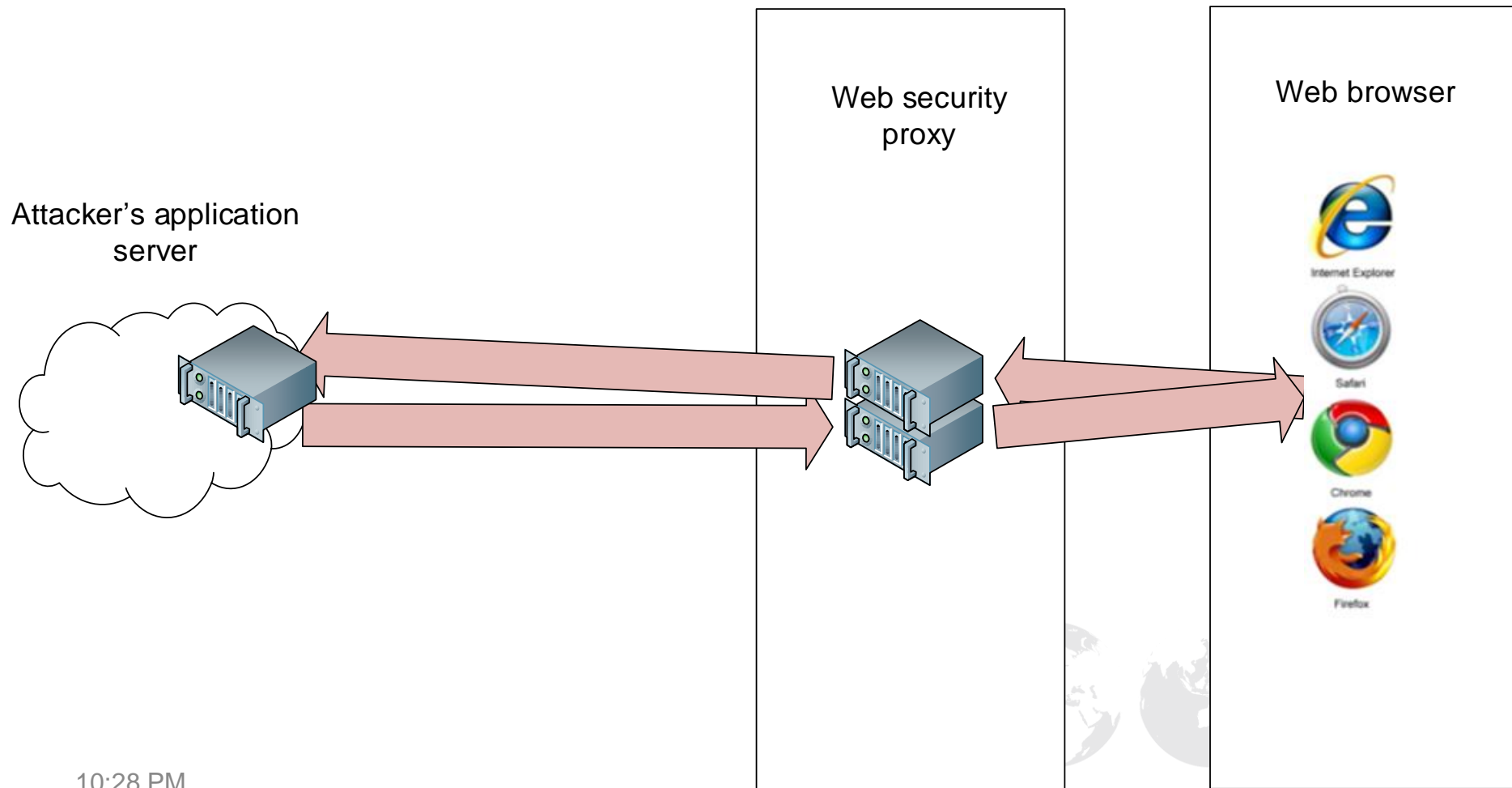
Via: 1.1 backup.xxxx.xxx.xx:3128 (squid/2.7.STABLE9)

X-Cache-Lookup: MISS from xxxxxx:53128, MISS from pfsense:3128

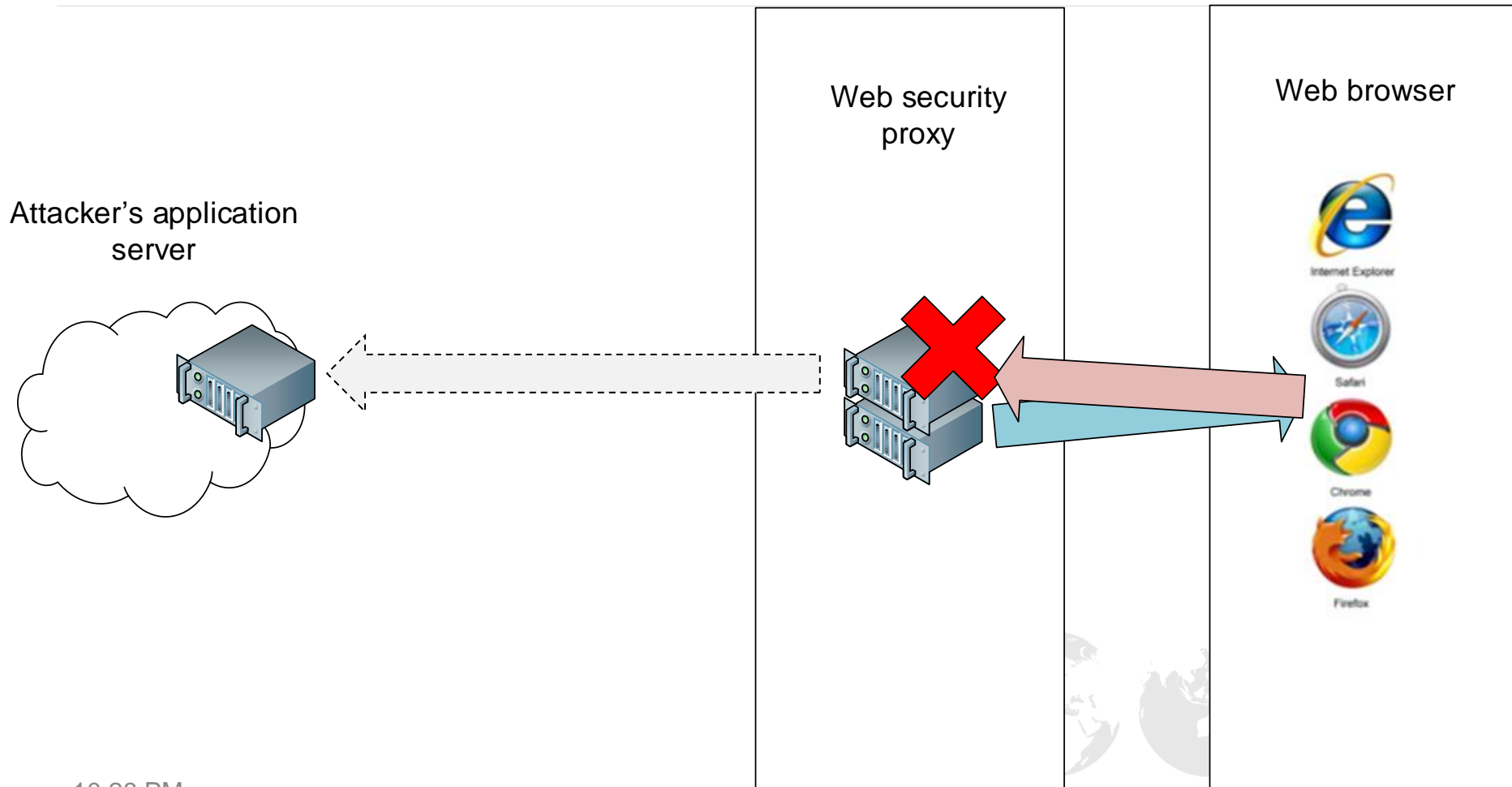
X-WebMarshal-RequestID: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX



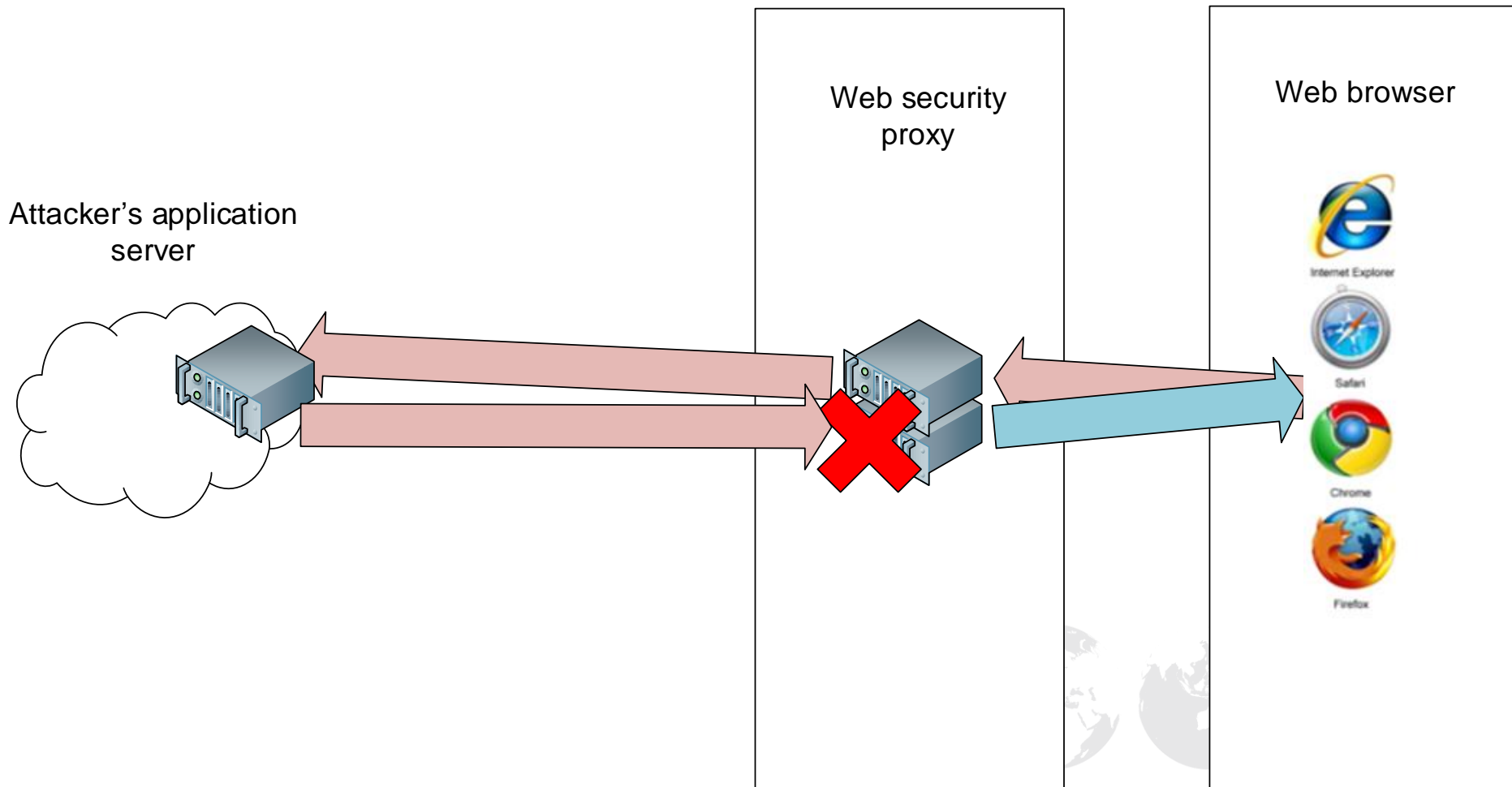
File Download Policy Enumeration



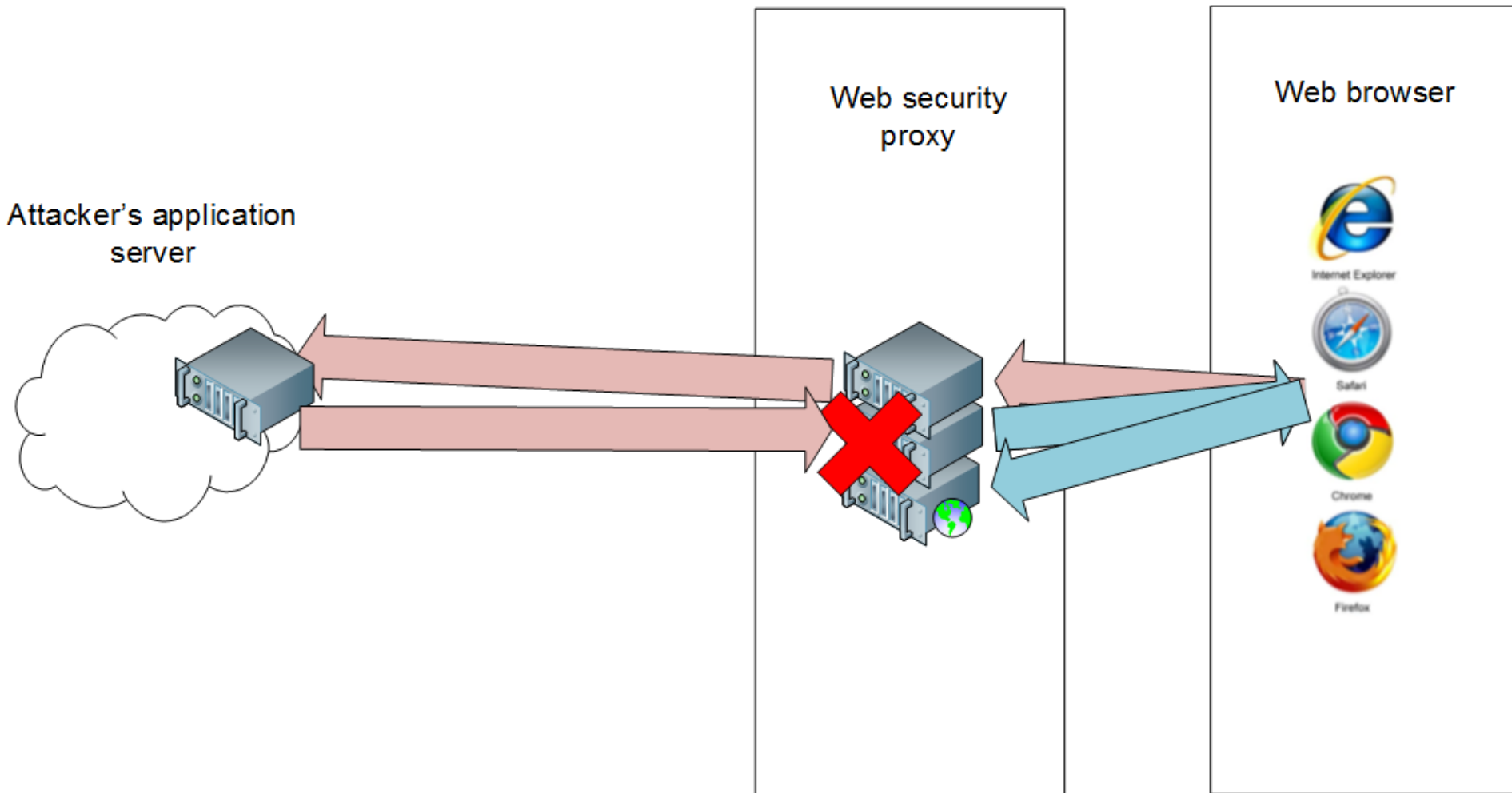
Blocking Request



Blocking Response



A Redirect Response



This Page Cannot Be Displayed

Based on your organization's access policies, this web site ([http://\[REDACTED\]/WebFEETstats/payloads/eicar.com](http://[REDACTED]/WebFEETstats/payloads/eicar.com)) has been blocked because it has been determined to be a security threat to your computer or the organization's network. Malware threat EICAR-AV-Test in the category Trojan Horse has been found on this site.

If you have questions, please contact your corporate network administrator and provide the codes shown below.

Date: Mon, 21 Jul 2014 14:59:37 EDT

Username: [REDACTED]

Source IP: [REDACTED]

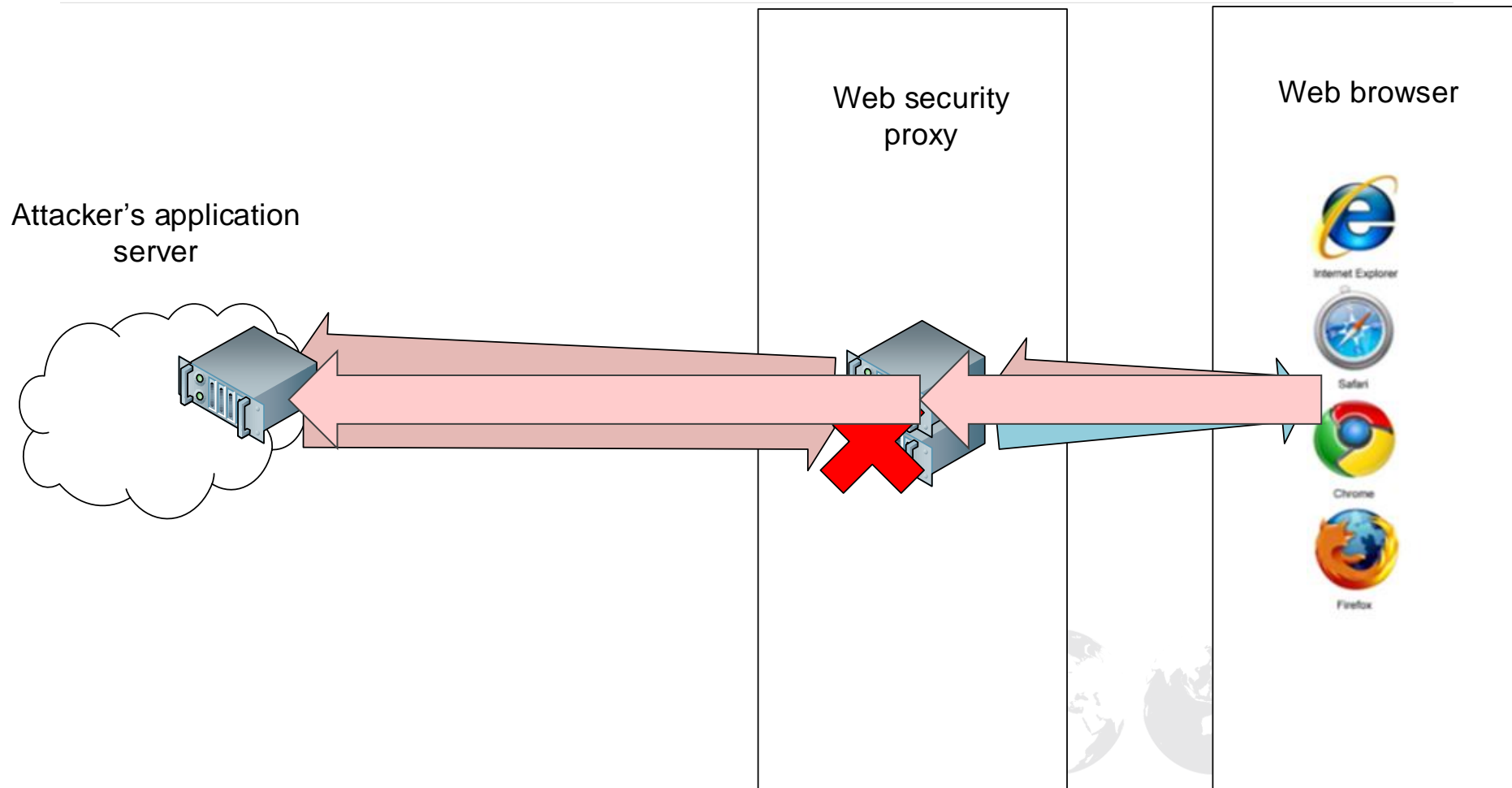
URL: GET [http://\[REDACTED\]/WebFEETstats/payloads/eicar.com](http://[REDACTED]/WebFEETstats/payloads/eicar.com)

Category: Uncategorized URLs

Reason: BLOCK-MALWARE

Notification: MALWARE_SPECIFIC

Fundamental Issue With Block-pages



Trend Micro OfficeScan Event

URL Blocked

The URL that you are attempting to access is a potential security risk. Trend Micro OfficeScan has blocked this URL in keeping with the network security policy.

URL: http://[REDACTED]WebFEETstats/payloads/eicar.com

Risk Level: Risk level cannot be displayed because active scripting is disabled.

Details:

Blocked by Web Reputation, Trend Micro OfficeScan 10.6 SP3,
Copyright © 1998-2013, Trend Micro Incorporated. All rights reserved.

Time: 13:09:41

Trend Micro has not yet checked the safety of the web site.

10:28 PM

What you can do:

Try visiting another site to find the information you want.

Malicious Content Blocked

Location: [REDACTED] /WebFEETstats/payloads/eicar.com

The requested location contains malicious content, identified as [EICAR-AV-Test](#) and was blocked from downloading.

sophos web protection

object is infected by [EICAR-Test-File](#)

Copyright © 2006

Message generated: 3:38:23 PM



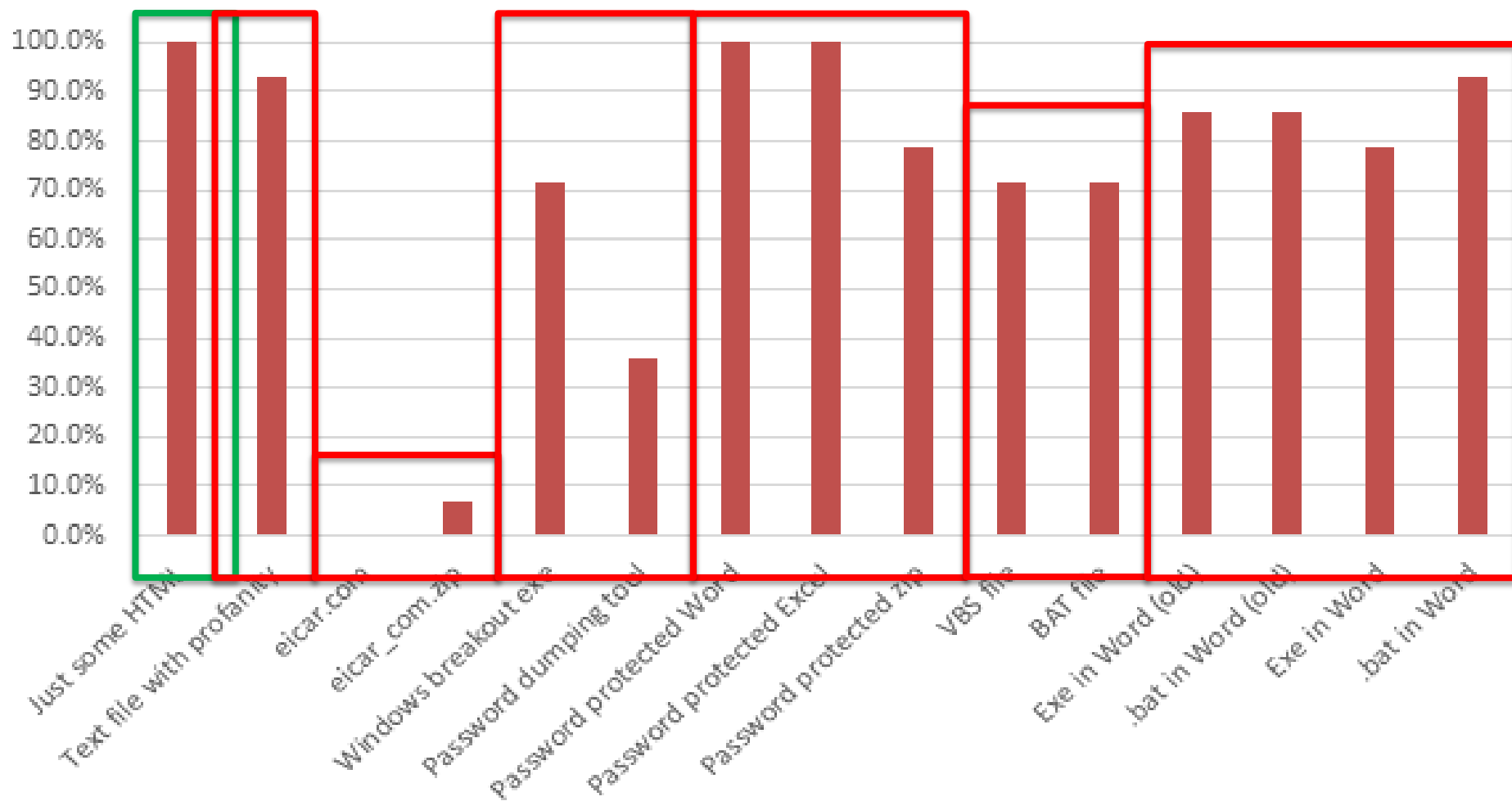
Example WebFEET Report

- Demo: Show a WebFEET reports



Example Download Test Statistics

Successful download by type

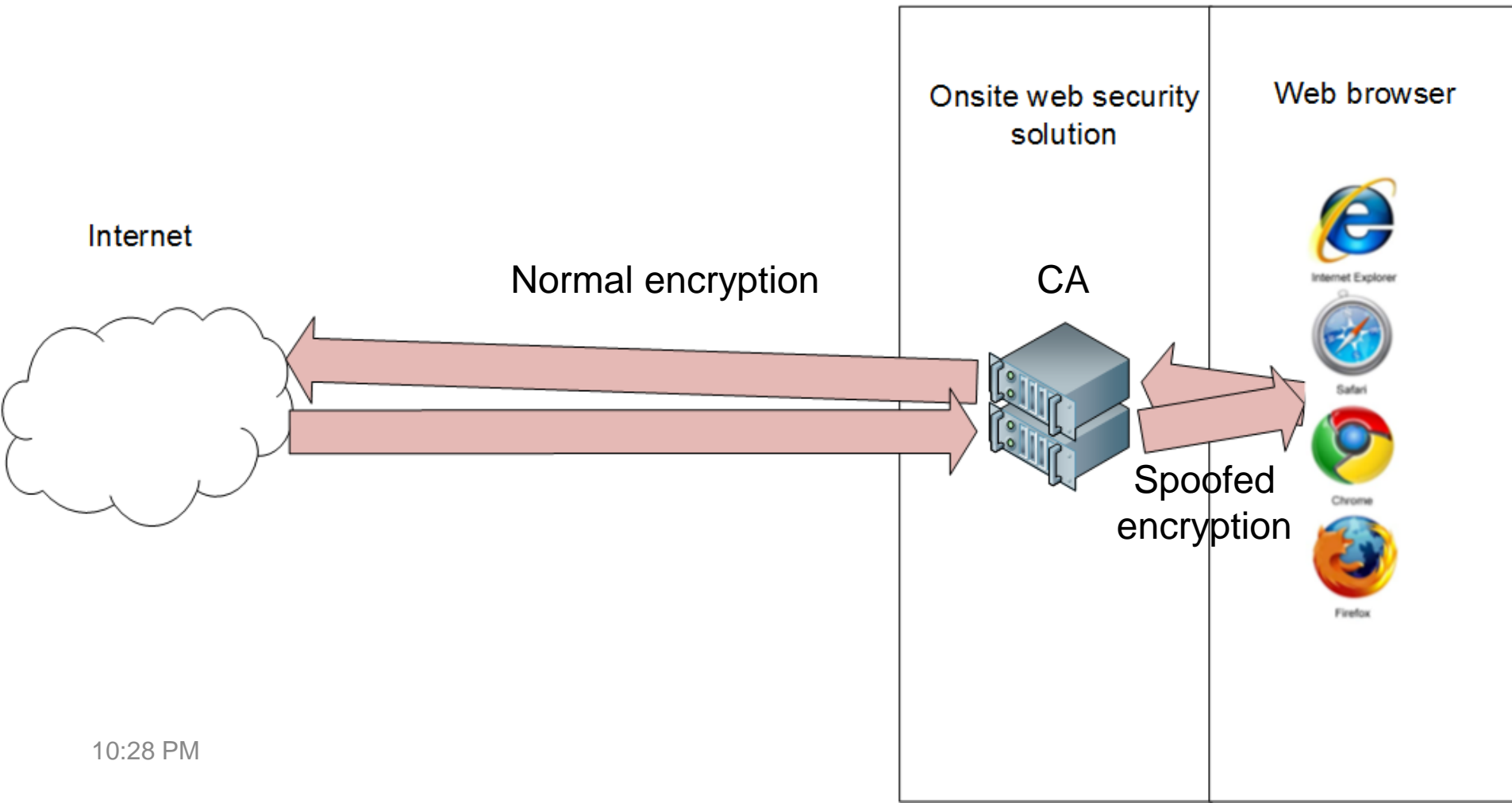


HTTP vs. HTTPS

- An effective HTTP policy can be irrelevant – because HTTPS interception and filtering are rare
- Even where HTTPS interception is present, there are usually plenty of policy bypasses



HTTPS Inspection



WebFEET HTTP vs. HTTPS

Basic Download Block Tests

Simple threats are tested here, to see if they are allowed, dropped, redirected, or result in a block-page.



Test File	Size	Result
EICAR basic test	68 bytes	Downloaded: Size = 68
A standard Windows exe	0.2 MB	Downloaded: Size = 187513
A file with profanity	39 bytes	Downloaded: Size = 39
An unlocked breakout shell	0.3 MB	Downloaded: Size = 342854
A Password dumping tool	0.5 MB	Downloaded: Size = 548715
EICAR in a zip	184 bytes	Downloaded: Size = 184
Some VBS script	22 bytes	Downloaded: Size = 22
A batch file	11 bytes	Downloaded: Size = 11



HTTPS Certificate Validation Issues

HTTPS Certificate Handling Enumeration (Correct Certificates)



Some of these are on non-standard ports, so some proxies may block these because of that (failure to load suggests filtering of non-standard ports, and may make some of the tests below invalid).

Category	Test Website	Image	Result
Valid Certificate	www.google.com (HTTPS)		Not Blocked
Valid Certificate	testssl-valid-r2i1.disig.sk:2444		Not Blocked

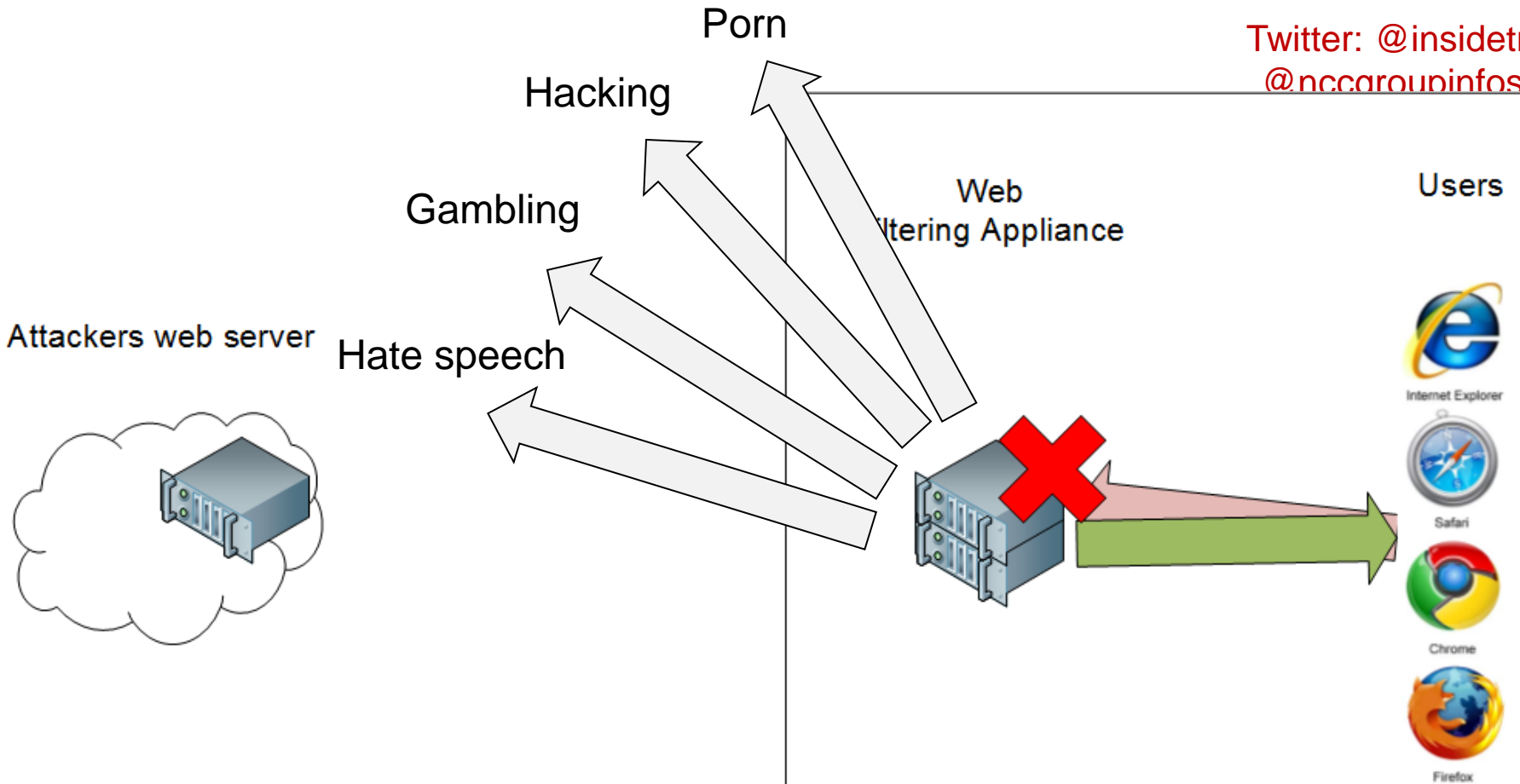
HTTPS Certificate Handling Enumeration (Incorrect Certificates, these should not load)

























If these resources load, this may be a result of an SSL break at the proxy (SSL MitM) in order to do HTTPS data inspection. This may also be causing external locations with invalid certificates to appear valid to the internal user.

Some of these are on non-standard ports, so some proxies may block these anyway (false negative for invalid certs).

Category	Test Website	Image	Result
Expired Certificate	testssl-expire-r2i1.disig.sk:2445		Not Blocked
Revoked Certificate	testssl-revoked-r2i1.disig.sk:2446		Not Blocked





Category	Test Website	Image	Result
Adult Material	www.porn.com		Blocked
Adult Material	www.redtube.com		Blocked
Drugs	ilovesmokingweed.com		Not Blocked
Drugs	marijuana.com		Blocked
Gambling	www.betfred.com		Blocked
Gambling	www.ladbrokes.com		Blocked
Hacking	www.exploit-db.com		Not Blocked
Hacking	ha.ckers.org		Not Blocked
Job Sites	www.totaljobs.com		Blocked
Job Sites	www.newjobs.com		Not Blocked
Online Email	mail.google.com		Not Blocked
Online Email	www.hotmail.com		Blocked
Online Pharmacy	www.chemist-4-u.com		Not Blocked
Online Pharmacy	www.pharmacy2u.co.uk		Blocked
Personal Network Storage and Backup	www.dropbox.com		Not Blocked
Personal Network Storage and Backup	pastebin.com		Not Blocked
Racism and Hate	www.chimpout.com		Blocked
Racism and Hate	www.stormfront.org		Blocked
Tasteless	www.4chan.org		Blocked
Tasteless	www.stupidness.com		Blocked
Violence	rotten.com		Blocked
Violence	www.liveleak.com		Blocked
Weapons	www.guns.com		Blocked
Weapons	www.bulkammo.com		Not Blocked

So For Web Filtering, I Know:

- What products you are using
 - Sometimes exact versions
- What your policy is for a wide variety of file downloads
- Whether you can detect threats in HTTPS
- How effective your URL filtering is and what categories you block

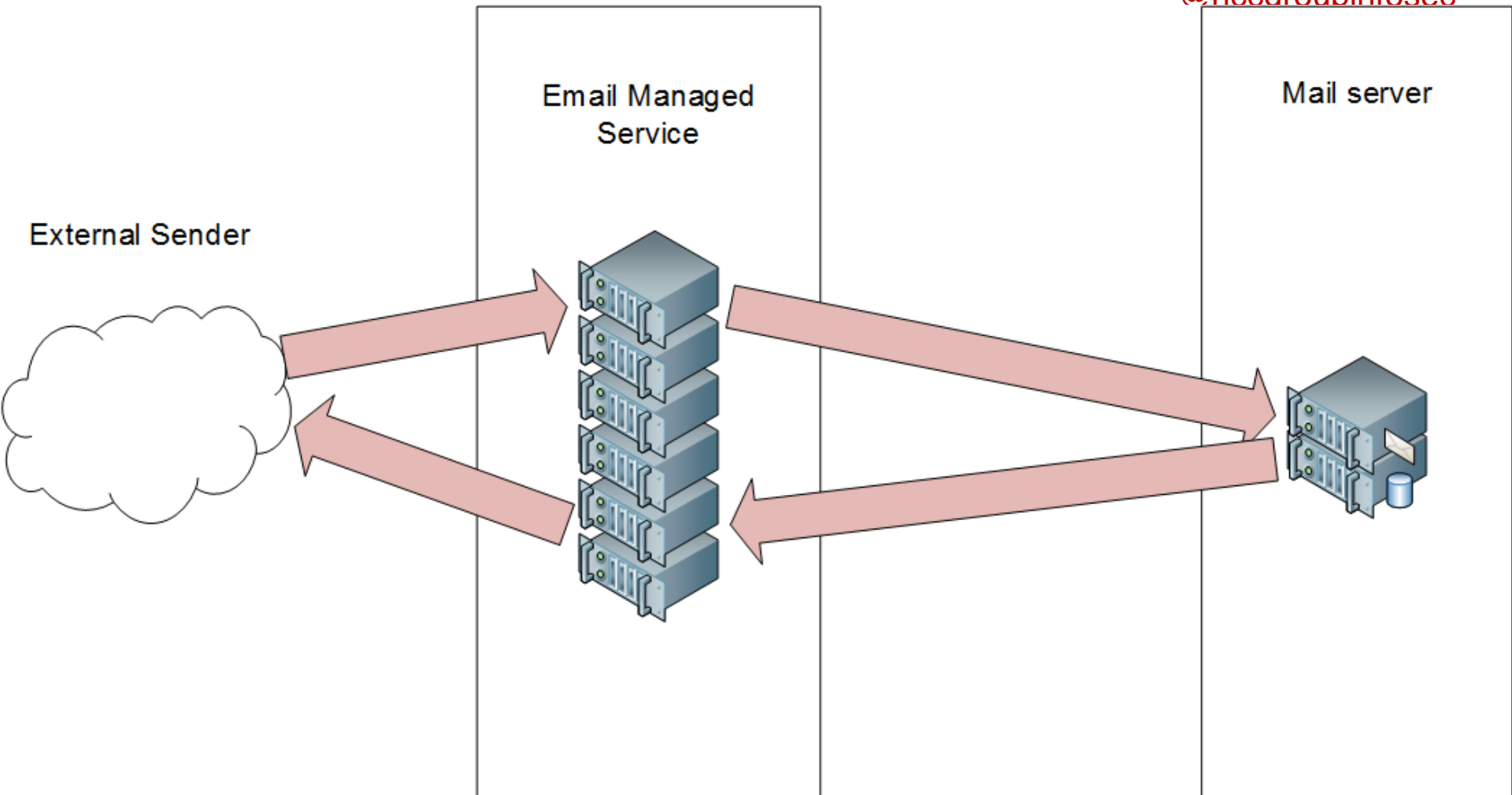
- All in under 10 seconds – no exploits required
 - Relatively transparent to the end user, but may be logs or alerts on the proxy

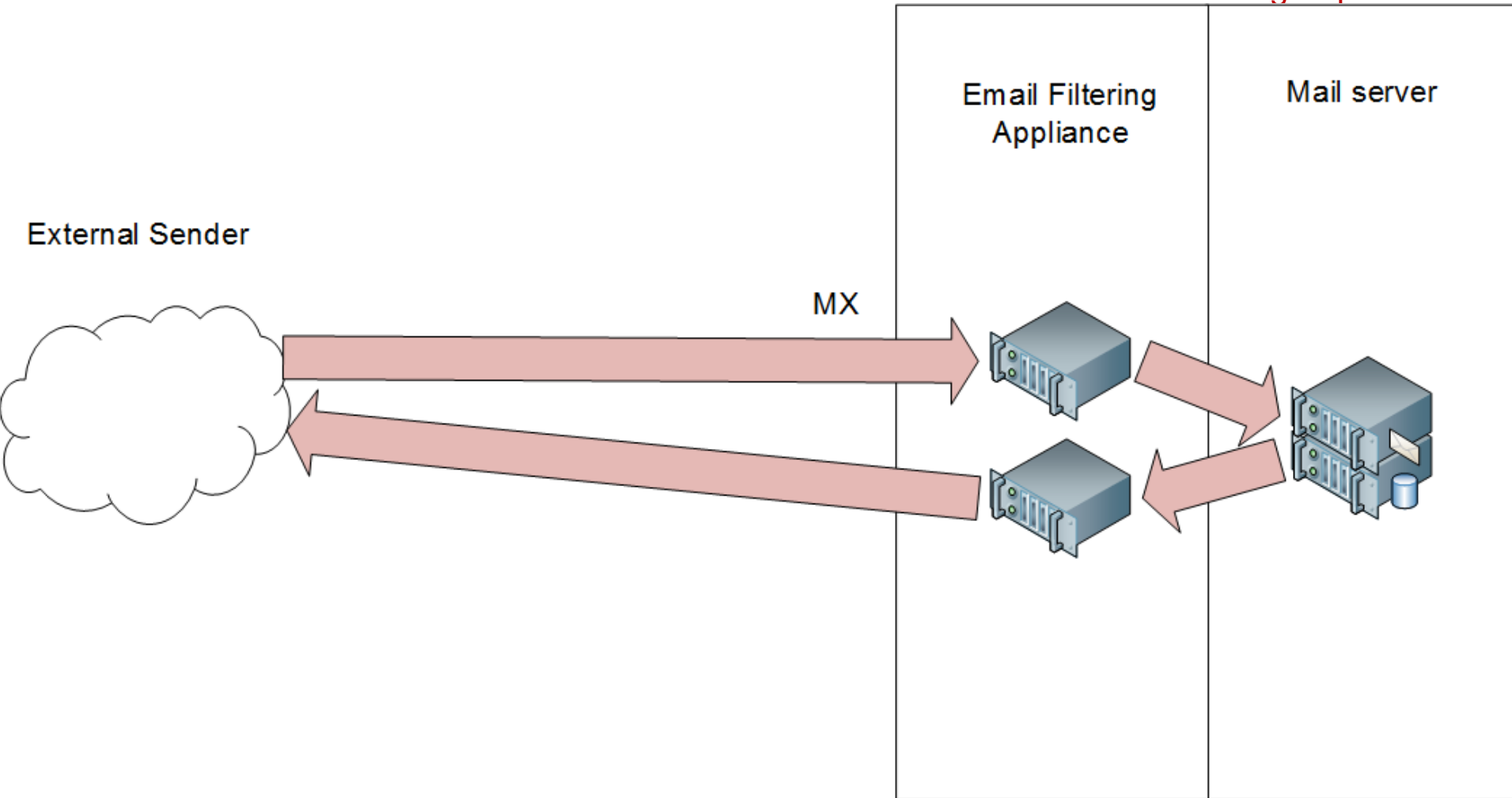


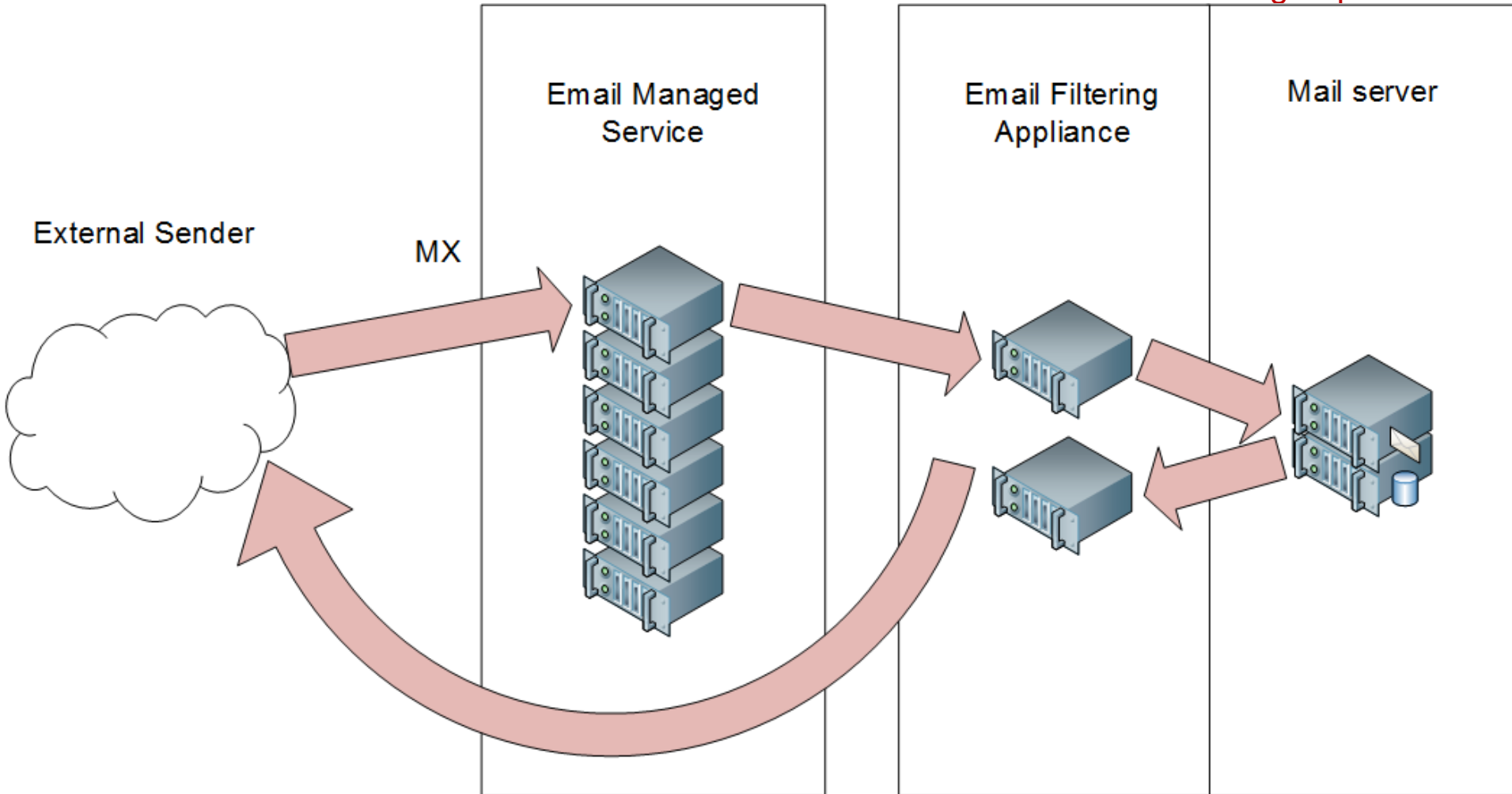
MailFEET

- Mail Filter External Enumeration Tool (MailFEET)
- Sends, receives test emails and parses responses
- Main components (python/sqlite)
 - Email sender/logger
 - Email bounce message collector/logger
 - Reporting tool
- For audits and reconnaissance

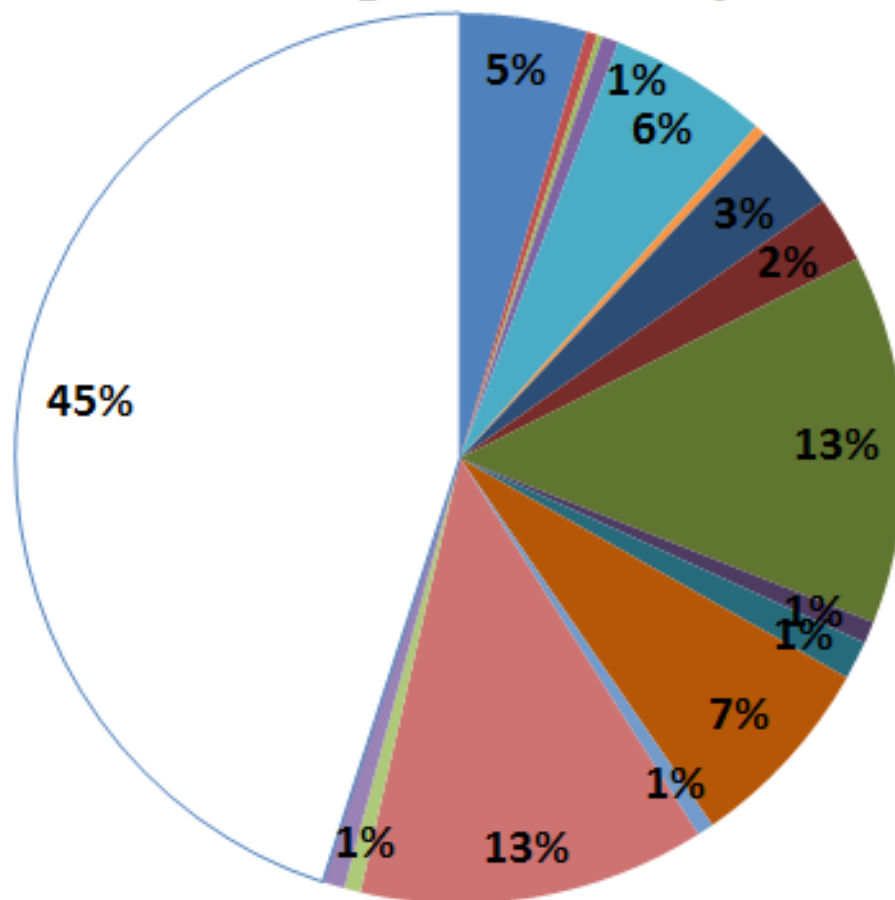








Fortune 500 managed services by MX record



- Cisco IronPort
- Google
- Microsoft
- Mimecast
- Sprint
- WebSense

- Dell MessageOne
- Google Postini
- Microsoft FrontBridge
- Mxlogic
- Symantec MessageLabs
- No identifiable service

- GoDaddy
- Google Mail
- Microsoft Outlook
- Proofpoint
- Trend Micro

X-IronPort-AV: E=Sophos;i="4.93,874,1378872000";

d="scan'208";a="37801415"

Received: from unknown (HELO [REDACTED]) ([REDACTED])

by [REDACTED] with ESMTP; 11 Dec 2013 17:48:43 -0500

Received: from localhost by [REDACTED];

11 Dec 2013 17:48:43 -0500

Message-Id: <431a6c\$[REDACTED]>

Date: 11 Dec 2013 17:48:43 -0500

To: [REDACTED]

From: "Mail Delivery System" <MAILER-DAEMON@bounce.email.[REDACTED]>

Subject: Delivery Status Notification (Failure)

MIME-Version: 1.0

Content-Type: multipart/report; report-type=delivery-status; boundary="tTZ0q.4xKe7+PZZ.1GJWag.1vpGZqL"

--tTZ0q.4xKe7+PZZ.1GJWag.1vpGZqL

content-type: text/plain;

charset="iso-8859-1"

Content-Transfer-Encoding: quoted-printable

The following message to <[REDACTED]> was undeliverable.

The reason for the problem:

5.x.0 - Message bounced by administrator

--tTZ0q.4xKe7+PZZ.1GJWag.1vpGZqL

content-type: message/delivery-status

Reporting-MTA: dns; [REDACTED]

Final-Recipient: rfc822; [REDACTED]

Action: failed

Status: 5.0.0 (permanent failure)

Diagnostic-Code: smtp; 5.x.0 - Message bounced by administrator (delivery attempts: 0)

--tTZ0q.4xKe7+PZZ.1GJWag.1vpGZqL

content-type: message/rfc822

X-sendergroup: InternetMailGateways

X-InvalidGSAddress:

Received: from [REDACTED] ([REDACTED])

by mxpcd01-public.ny.fw.gs.com with ESMTP; 11 Dec 2013 17:48:43 -0500

X-IronPort-AV: E=Sophos;i="4.93,874,1378872000";

d="doc'32?scan'32,208,32";a="22206633"

Received: from mx0a-0014b501.pphosted.com ([67.231.148.165])

by [REDACTED] with ESMTP/TLS/DHE-RSA-AES256-SHA; 11 Dec 2013 17:48:43 -0500

Received: from pps.filterd (m0000325.pops.net [127.0.0.1])

> by mx0a-0014b501.pphosted.com (8.14.5/8.14.5) with SMTP id rBBMcfwg009609

> for [REDACTED]; Wed, 11 Dec 2013 17:48:42 -0500

Received: from [REDACTED] ([REDACTED])

> by mx0a-0014b501.pphosted.com with ESMTP id lgpwecrwax-1

> (version=TLSv1/SSLv3 cipher=AES256-SHA bits=256 verify=NOT)

> for [REDACTED] Wed, 11 Dec 2013 17:48:41 -0500

Message-ID: <25864.3069277866-sendEmail@mail2>

From: "[REDACTED]" <[REDACTED]>

To: "[REDACTED]" <[REDACTED]>

Subject: Test message - please ignore (script) 7d34aa0d

Date: Wed, 11 Dec 2013 22:48:41 +0000

X-Mailer: sendEmail-1.56

MIME-Version: 1.0

Content-Type: multipart/mixed; boundary="----MIME delimiter for sendEmail-962038.712416874"

X-Proofpoint-Virus-Version: vendor=fsecure engine=2.50.10432:5.11.87,1.0.14,0.0.0000

definitions=2013-12-11_05:2013-12-11,2013-12-11,1970-01-01 signatures=0

X-Proofpoint-Spam-Details: rule=notspam policy=default score=0 kscore.is_bulkscore=0

kscore.compositescore=0 circleOfTrustscore=0

compositescore=0.999311915122763 urlsuspect_oldscore=0.999311915122763

suspectscore=2 recipient_domain_to_sender_totalscore=0 phishscore=1

bulkscore=0 kscore.is_spamscore=0 recipient_to_sender_totalscore=0

recipient_domain_to_sender_domain_totalscore=0 rbsscore=0.999311915122763

spamscore=0 recipient_to_sender_domain_totalscore=0 urlsuspectscore=0.9

adultscore=0 classifier=spam adjust=0 reason=mlx scancount=1

engine=7.0.1-1305240000 definitions=main-1312110138

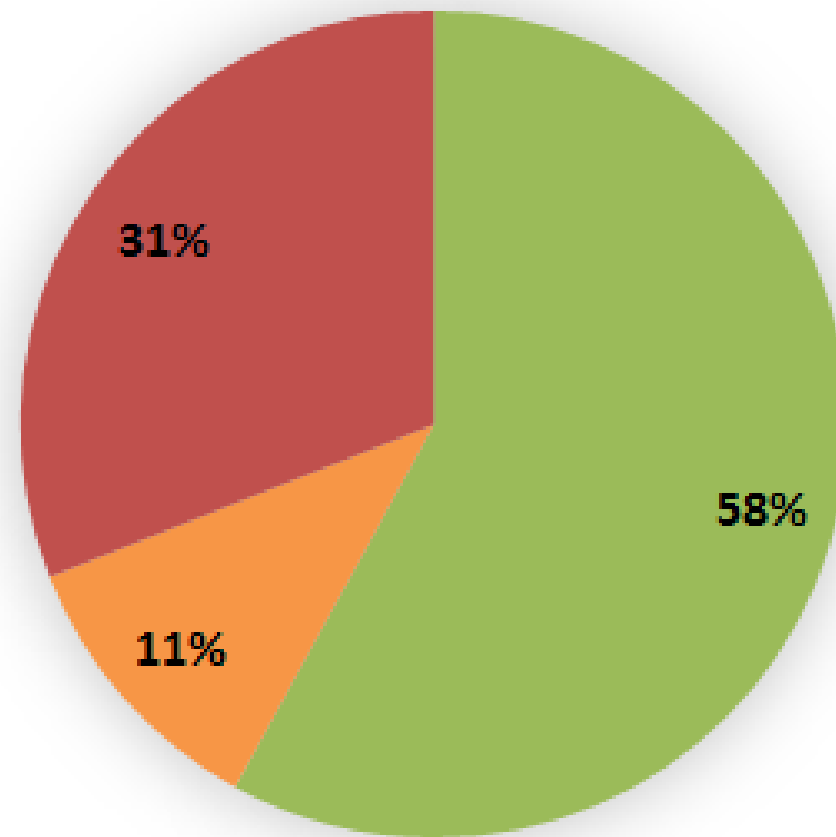
--tTZ0q.4xKe7+PZZ.1GJWag.1vpGZqL--

Product disclosure examples

- X-IronPort-AV: E=Sophos;i="4.93,874,1378875600";
- MailMarshal (v7,1,0,4874)
- X-Proofpoint-Spam-Details: rule=notspam
policy=default score=41 spamscore=0 ndrscore=41
suspectscore=3 adjustscore=0 phishscore=0
adultscore=0 bulkscore=0 classifier=spam adjust=0
reason=mlx scancount=1 engine=7.0.1-1305240000
definitions=main-1308150307



Fortune 500 non-existent recipient acceptance



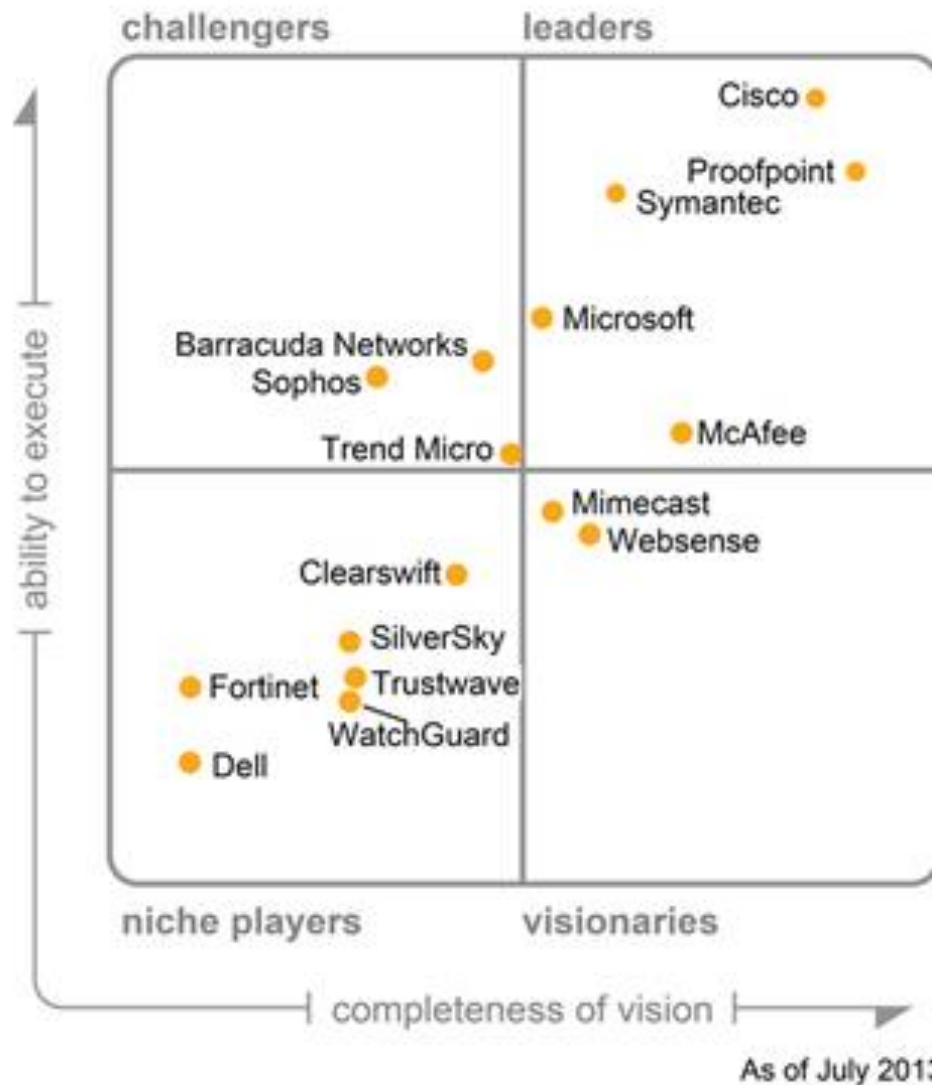
■ Didn't accept ■ Accepted ■ Accepted and replied

Enumerating products in use

- Create signatures for:
 - X-Headers
 - Received headers
 - Message body/attachments
 - Hostnames



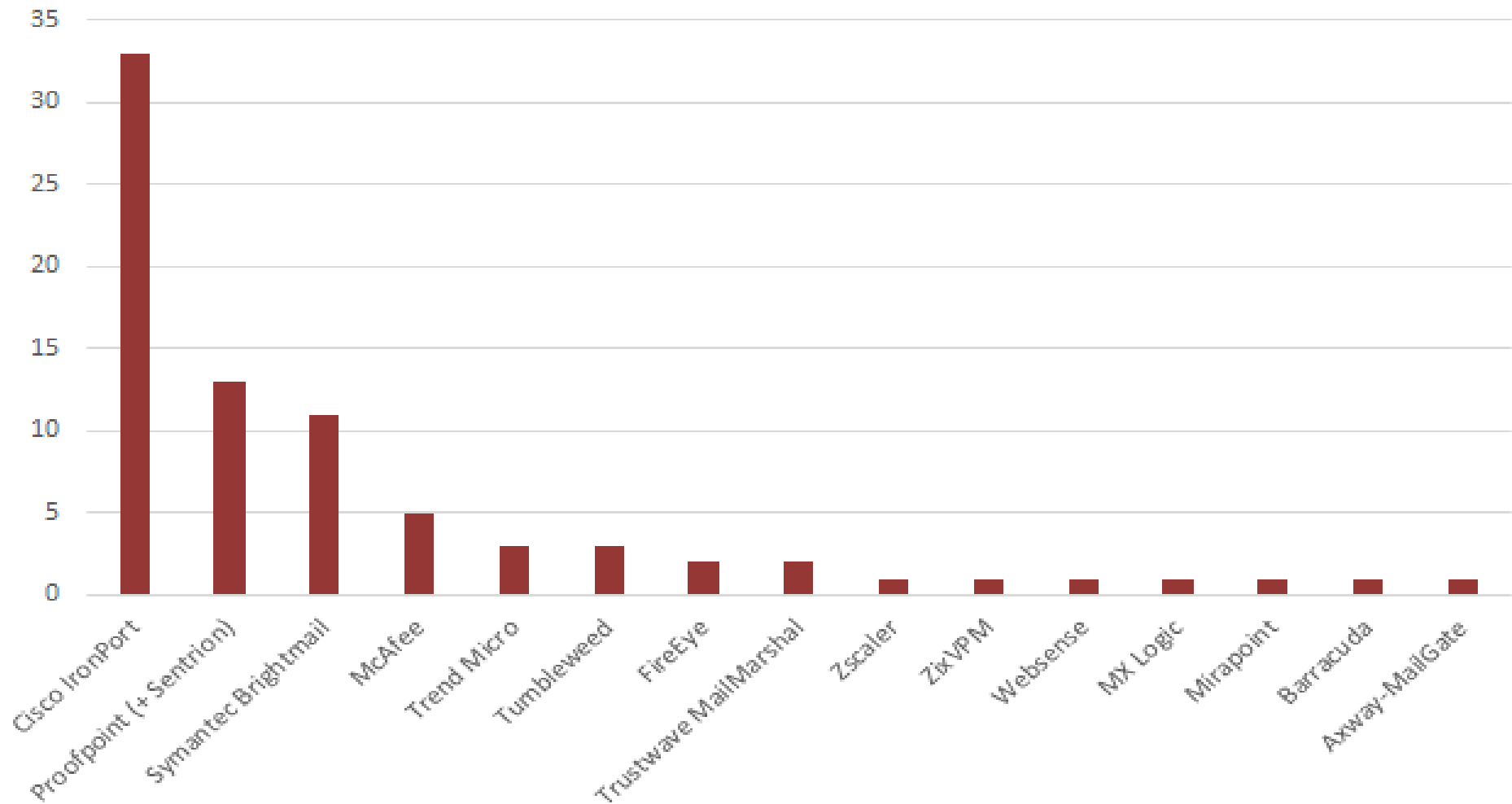
Figure 1. Magic Quadrant for Secure Email Gateway



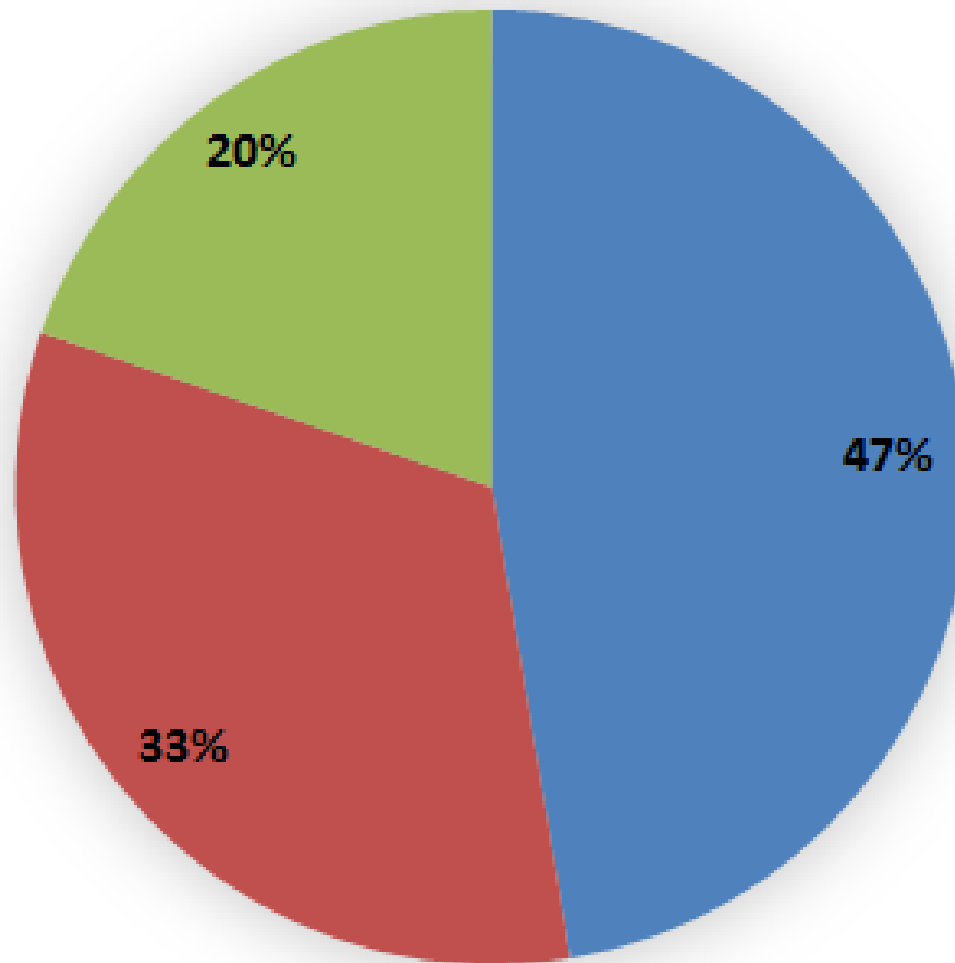
Source: Gartner (July 2013)



Email filter appliance product type by vendor (enumeration via bounce message analysis)



Email filtering managed service vs. product for 152 leading organisations



■ Manage service

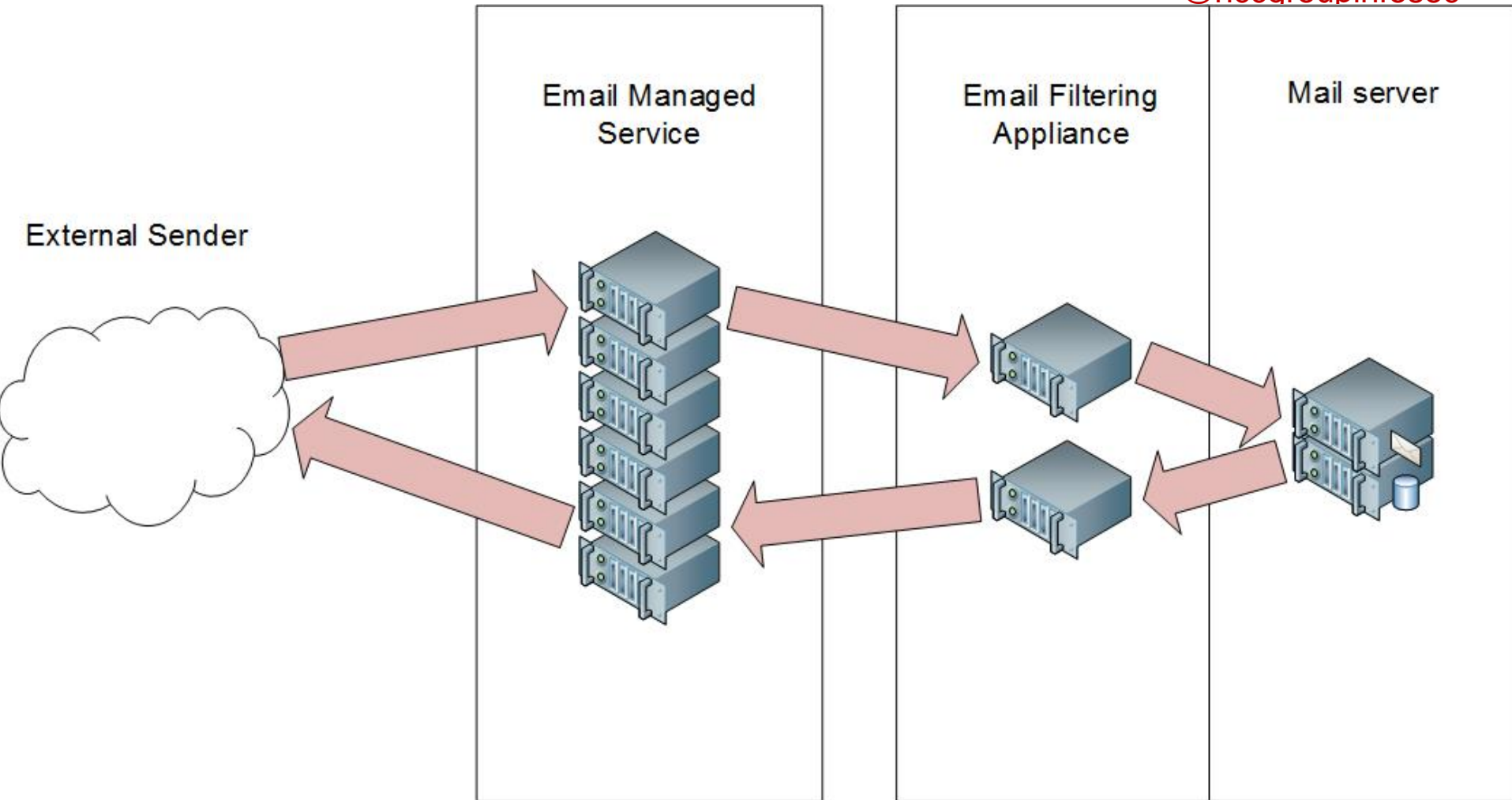
■ Just product (mainly appliances)

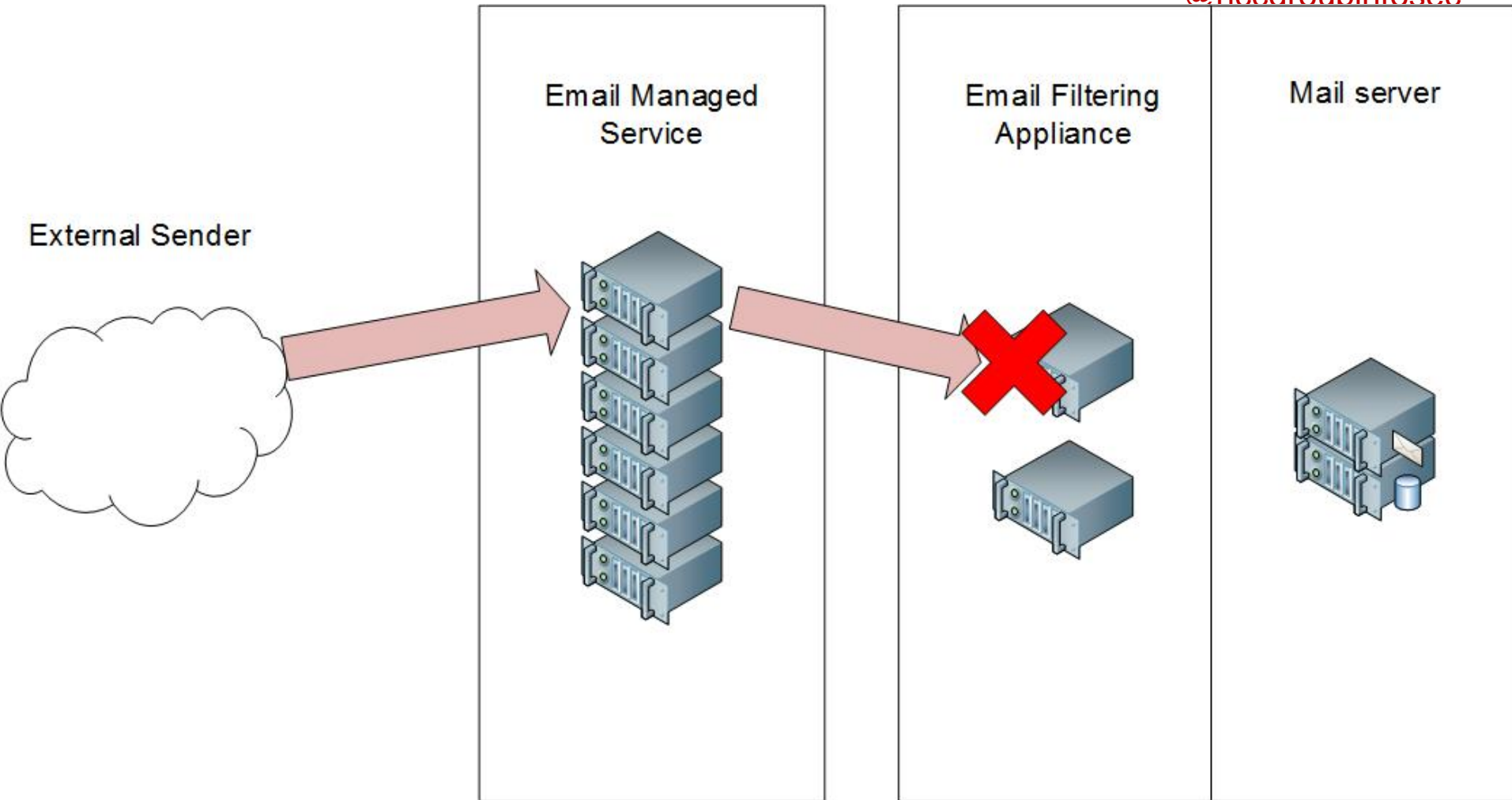
■ Both service and product

Policy enumeration

- Send 4 different test messages, to each MX record, of 152 domains – you get 2,500 responses – what happened?
 - Simple text message (no threat)
 - Exe embedded in a Word (2010) document
 - Password protected Excel spreadsheet
 - VBS in Word (2003) document



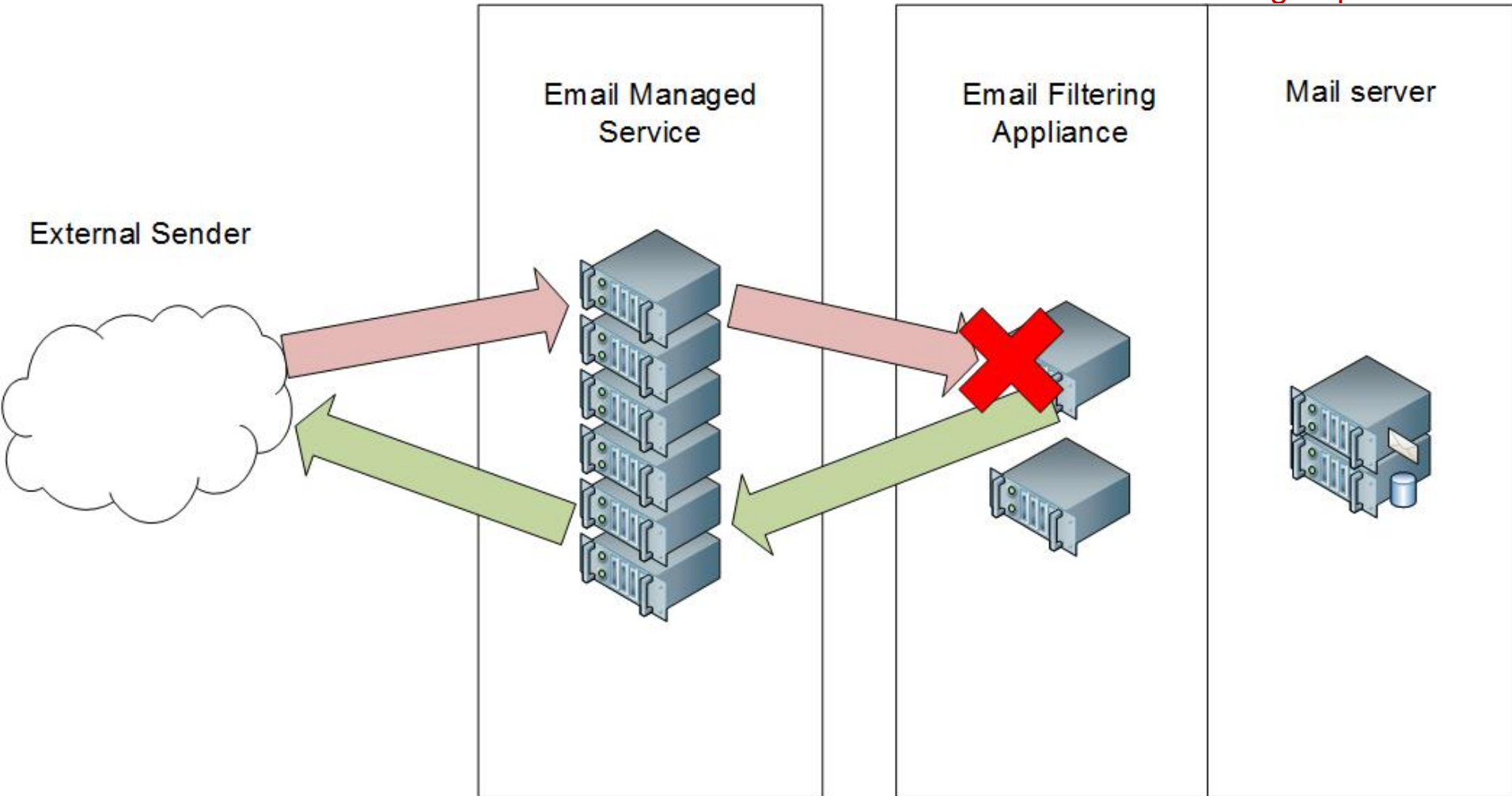




Types of message you can get back

- Delivery Service Notifications (DSN)
 - Non-delivery report (NDR) “550: Recipient does not exist”
 - Policy block informational messages
 - Message quarantined
 - Message corrupt (could not be processed)
 - Message delayed
- Out of office messages
 - Contain useful user information

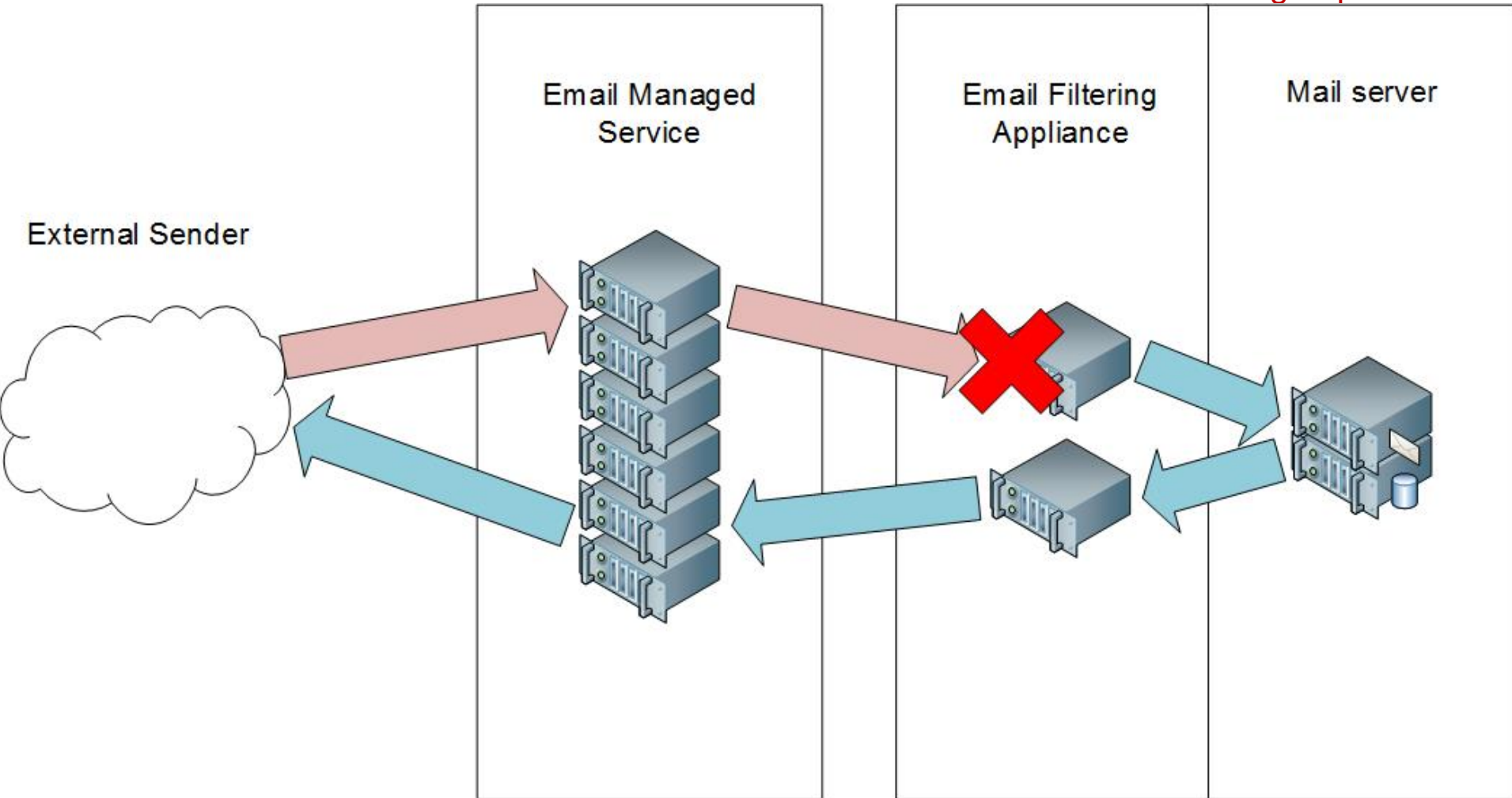




Classic disclosure (“block” message)

“A message or attachment you have sent to <Company name> has been filtered. Please use a different file format or place your attachment in a password protected ZIP file and resend the message.”





Message modification examples

McAfee®

Symantec Mail Security replaced exe-in-word-2010.docx with this text message. The original file contained a filtering violation and was quarantined.

::

Information.

Rule: 'Blocked Files'
Context: '[untitled]'
Disallowed due to format

See your system administrator for further information.

Copyright © 1993-2013 McAfee, Inc.
All Rights Reserved.
<http://www.mcafee.com>



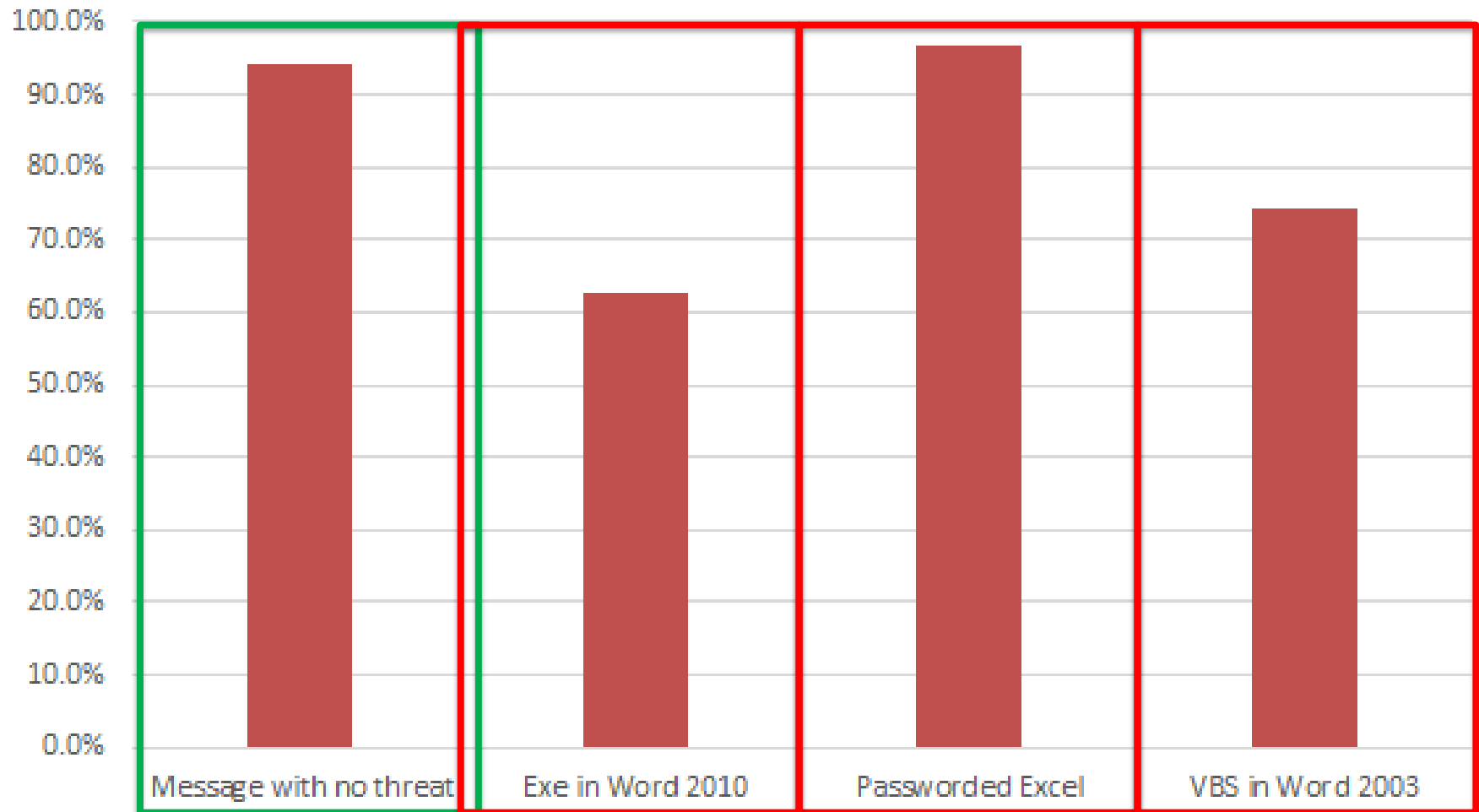
Need to quickly classify bounces

- Which are bounces from the mail-server?
 - Which have the original message?
 - Which have the original attachment?
- Which are “block notification” messages?
- Which are “other” types?

- Criteria
 - Checksum original attachment, message size, number of received headers, X-headers, structure, attachments, specific text strings



Small four message test set



Policy enumeration for NCC clients

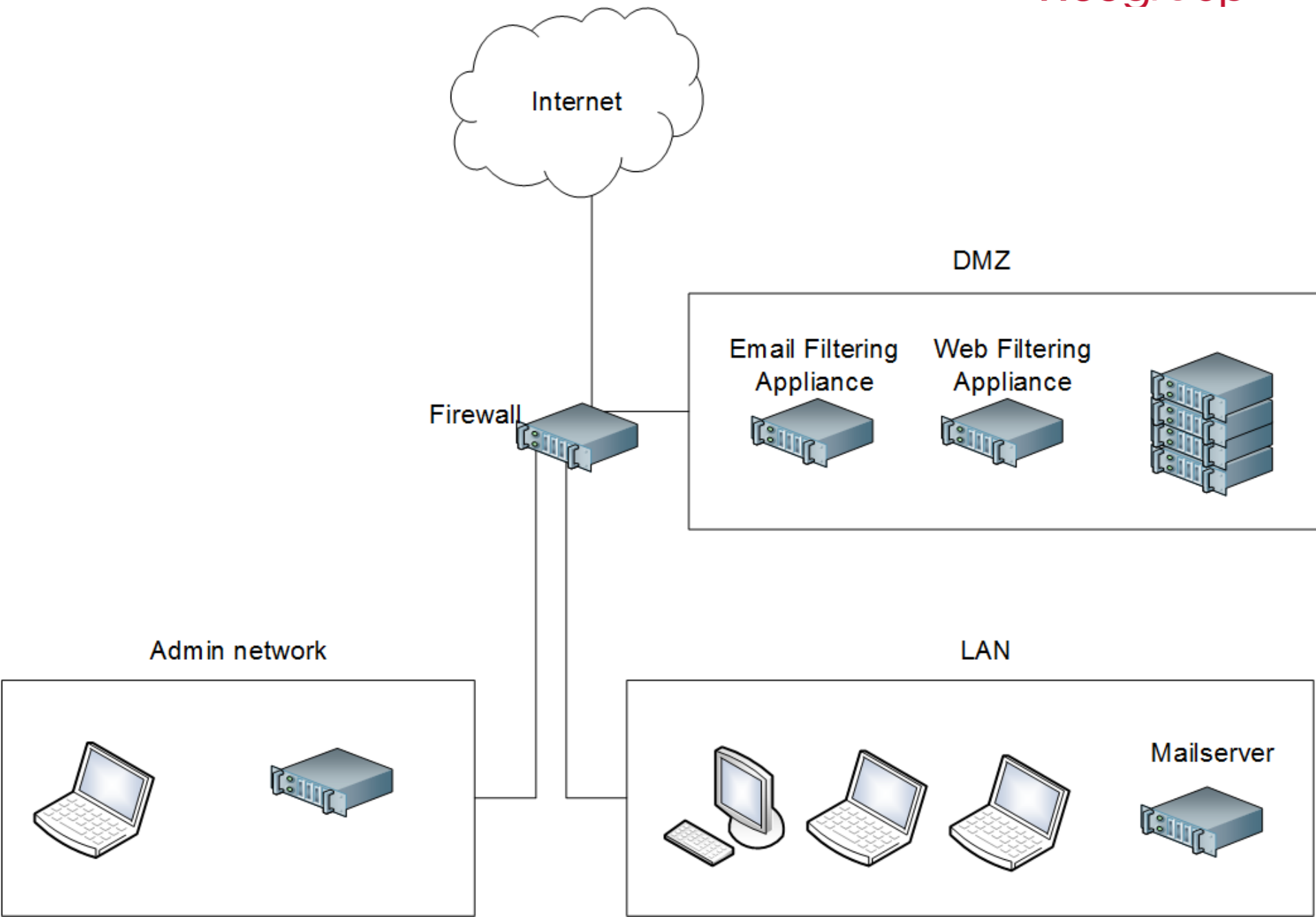
- Demo: Show example report
- Demo: Show example document with payload



So For Email Filtering, I Know:

- What products and services you are using
 - Often with exact versions
- What your policy is for a wide variety of file attachments
- Typically between 5 minutes to 1 hour for 50 attachments
 - Multiple MX records and multiple message paths
 - Often transparent to the end user, but may messages quarantined on email filter





Attacks which work

- HTTPS for the Win!
- Hidden payloads requiring “Deep content analysis”
 - Exes and scripts in Word Doc, PowerPoint, Excel etc.
 - Exe and scripts in Zips
 - PowerShell in HTA files or Document macros
 - Multiple layers: Exe in Zip in Documents.
 - Payloads in password protected documents and archives
 - 1000s of potential tests



run_this.exe



Summary

- External attackers can enumerate products and policy
- Policies are generally weak
 - No 0-Day required
 - Encryption is the attacker's friend
 - Embedded threats were rarely detected



Resources

- Updated presentation slides
- Whitepaper on web enumeration
- Whitepaper on email enumeration

- WebFEET tool
- MailFEET tool





UK Offices

Manchester - Head Office
Cheltenham
Edinburgh
Leatherhead
London
Thame

European Offices

Amsterdam - Netherlands
Munich – Germany
Zurich - Switzerland



North American Offices

San Francisco
Atlanta
New York
Seattle



Australian Offices

Sydney